REMARKS

In the Office Action, the Examiner rejected Claims 1-43, which are all of the pending claims, under 35 U.S.C. §103 as being unpatentable over U.S. Patent 6,453,296 (Iwamura) in view of a document "Introducing Trusted Third Parties..." (Wilhelm, et al.). Claims 10-14, 16, 17, 22, 28, 29, 30, 34 and 39 and the intervening claims were further rejected under 35 U.S.C. §112 as being indefinite. In addition, the Examiner noted several informalities in the specification and the abstract, objected to the lack of indentations in Claims 1, 31, 34 and 40, and required correction of these matters.

With regard to the specification, Applicants are herein re-phrasing page 4, line 25 and page 17, line 2. the former now states that "all the client can know for sure is the identity of the entity," and the latter now avoids the double use of "that." Also, the spelling of "server" has been corrected on line 18 of the abstract, and this opportunity is being taken to indent the subparagraphs of several claims, including Claims 1, 31, 34 and 40.

In view of the foregoing, the Examiner is asked to reconsider and to withdraw the objections to the abstract and the specification and the objection to the lack of indentations in the claims.

With respect to the rejection of claims under 35 U.S.C. §112, Claims 10-14, 16, 17, 22, 28 and 30 are being amended to more positively set forth several features. In particular, in these claims, the reference to "said current co-server state and said inputs" is being changed to "a current co-server state and inputs." It is believed that these claims now appropriately introduce these limitations.

Claim 17 is being amended to change "a portion of the decryption" to "a portion of a decryption," which is believed to better introduce this feature of the claim. Claims 10, 16, 29, 34 and 39 are also being amended to delete the "such as" clauses.

In the Office Action, the Examiner objected to Claim 30 on the basis of the language "the output returned to client." Applicants Attorneys have carefully reviewed Claim 30, and this language does not occur in the claim. It is noted that this claim a message M that is sent back to the client, however, there is a clear antecedent basis for all of these terms.

Applicants believe that the above-discussed changes fully address the above-identified rejection of the claims as being indefinite, and the Examiner is thus respectfully requested to reconsider and to withdraw this rejection of the claims under 35 U.S.C. §112.

With respect to the rejections of the claims under 35 U.S.C. §103, these claims patentably distinguish over the prior art because the references do not show or suggest the use of a trusted co-server in the manner described in independent Claims 1, 31, 33, 34, 37 and 40.

More specifically, this invention teaches a way that, operating within the existing SSl and Web infrastructure, a sever operator can provide services with security properties that a remote user can verify – even if the server operator may have motivation to subvert these properties.

Regarding Iwamura, this reference teaches a special-purpose distributed system to support a particular agency's commerce applications. The system uses shared secrets and has the agency distribute secret keys (col 4), which makes it impossible for the parties involved to prove non-repudiation. Furthermore, there is no means involved for any party to verify that the information at the other end is protected and properly assembled, nor to prove these properties to a third party.

Indeed, the only real resemblance to the present invention is this invention's preferred use of SSL and the Web, to produce a distributed system with encrypted connections. However, SSL and the Web comprises an existing, universal, multi-application infrastructure, not bound to an agency; the cryptography is public-key; the keypairs are generated at local nodes, not provided by the remote agency.

Regarding "tamper-resistant hardware," Applicants respectfully disagree with the Examiner's argument that combining ideas like Iwamura with tamper-resistant hardware would have been "obvious." A key building block of this invention is that application software loaded into such hardware can turn around and prove itself (that it is that software, running inside untampered hardware) to arbitrary third parties using public-key cryptography. (This is discussed on Pages 16-17 of the present application, which refer to the process necessary to go from "tamper resistant hardware" to this broader property. In addition, this invention, in its preferred embodiment, is able to prove itself within the current SSL infrastructure, via indirection through a standard CA, and thus letting a user equipped with a standard browser to make the appropriate trust judgment.

Regarding Wilhelm, this reference, similar to this invention, is based on the idea of using tamper-resistant hardware with a manufacture-certified keypair. However, Wilhelm uses this keypair to enable a remote shipper of an agent to ship the agent encrypted to the hardware; once decrypted, the agent can use secrets it carried with it to authenticated back to the shipper. In contrast, the preferred implementation of this invention uses the keypair itself to authenticate the code that lives in the hardware. This approach lets the code arrive unencrypted, and lets the relying party (standard term for: the one who wants to make a trust judgment about some remote entity---the entity here being the executing code) be ANYONE, not just the remote shipper of the agent. Furthermore, the system of the present invention does not require mobile agents that move between agent hosts. Instead, this invention, preferably, uses static Web server applications, that interact with multiple remote parties using standard browsers, not special agent nodes.

Even if one of ordinary skill in the art were led to combine Wilheim and Iwamura, the present invention still would not have been obvious. In particular, even if one traces through how information flows between machines controlled by parties with competing interests, one finds none of this in Iwamura and only the vaguest resemblance in Wilhelm.

Independent Claims 1, 31, 33 and 40 each positively set forth the step of using a trusted co-server as a trusted third party in interactions between the client and the server. Independent Claim 34 is directed to a trusted co-server itself, and the claim positively describes the feature that the co-server is used so that parties can trust the correct execution of the co-server in interactions between the client and the server, despite attempts by a Web server to subvert this. Claim 37 defines a method of enhancing the security of a Web based transaction, and the claim describes the feature that the co-server carries out a function on inputs such that the parties trust interactions between the parties and the server.

The other references of record have been reviewed, and they too, whether considered individually or in combination, also fail t disclose or teach the use of the trusted co-server in the manner described in the above-claims.

For example, McDonough does not teach how the users can verify that the server operator is not lying or mistaken when the server operator claims the scanning has been performed.

This invention, as mentioned above, teaches a way that, operating within the existing SSL and Web infrastructure, a server operator can provide services with security properties that a remote user can verify---even if the server operator may have motivation to subvert these properties.

The present invention is a universal infrastructure that supports myriad applications from multiple server operators. The invention permits the additional flexibility of permitting the server operator, remote users, server application developers, hardware manufacturers, and SSL CAs all to be separate parties.

Because of the above-discussed differences between Claims 1, 31, 33, 34, 37 and 40 and the prior art, and because of the advantages associate with those differences, these claims patentably distinguish over the prior art and are allowable. Claims 2-30 are dependent from Claim 1 and are allowable therewith; and Claim 32 is dependent from, and is allowable with, Claim 31. Likewise, Claims 35 and 36 are dependent from Claim 34 and are allowable therewith; Claims 38 and 39 are dependent from, and are allowable with Claim 37; and Claims 41 and 42 are dependent from Claim 40 and are allowable therewith. The Examiner is, accordingly, respectfully asked to reconsider and to withdraw the rejections of Claims 1-42 under 35 U.S.C. §103, and to allow these claims.

Every effort has been made to place this case in condition for allowance. For the reasons set forth above, the Examiner is requested to reconsider and to withdraw the objections to the specification and the abstract and to the indentations in the claims. The Examiner is also asked to reconsider and to withdraw the rejection of Claims 10-14, 16, 17, 22, 28, 29, 30, 34 and 39 and the intervening claims under 35 U.S.C. §112, and the rejection of Claims 1-42 under 35 U.S.C. §103, and to allow Claims 1-42. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,

John S. Sensny
John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser
400 Garden City Plaza – Suite 300
Garden City, New York 11530
(516) 742-4343

LP:jy